



Payment Card Industry (PCI) Payment Application Data Security Standard

**Riepilogo delle modifiche dalla
versione PA-DSS 1.2.1 alla 2.0**

Ottobre 2010

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Aspetti generali	Aspetti generali	Attestato di convalida L'attestato di convalida è stato eliminato dall'appendice ed è stato creato un documento separato. Riferimenti del documento aggiornati di conseguenza.	Chiarimento
Aspetti generali	Aspetti generali	Scopo del documento Aggiunti riferimenti alle ulteriori risorse disponibili sul sito Web PCI SSC.	Ulteriori istruzioni
Aspetti generali	Aspetti generali	Relazione tra PCI DSS e PA-DSS <ul style="list-style-type: none"> ▪ Aggiunta frase per chiarire che l'uso della sola applicazione conforme agli standard PA-DSS non rende l'entità conforme agli standard PCI DSS. ▪ Chiarimento dei dati sulla striscia magnetica "e/o dati equivalenti sul chip." 	Chiarimento
Aspetti generali	Aspetti generali	Ambito del programma PA-DSS Chiarimento sul fatto che il programma PA-DSS non è valido per le applicazioni di pagamento sviluppate per un singolo cliente e vendute allo stesso per l'uso esclusivo del cliente in questione.	Chiarimento
Aspetti generali	Aspetti generali	Applicabilità degli standard PA-DSS alle applicazioni di pagamento a terminali hardware Aggiornata, ampliata, chiarita e cambiato il nome alla sezione per prendere in esame le applicazioni di pagamento a terminali hardware, nei casi in cui può essere possibile soddisfare i requisiti PA-DSS al di fuori dell'applicazione di pagamento.	Ulteriori istruzioni
Aspetti generali	Aspetti generali	Requisiti per PA-QSA Spostato "Il PA-QSA deve avere accesso a un laboratorio in cui viene eseguito il processo di convalida" dal laboratorio di test alla sezione dei Requisiti PA-QSA.	Chiarimento
Aspetti generali	Aspetti generali	Laboratorio di test Chiarite le posizioni dei laboratori di test e l'esigenza per il PA-QSA di convalidare l'installazione completa dell'ambiente del laboratorio.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Aspetti generali	Aspetti generali	<p>Informazioni sull'applicabilità degli standard PCI DSS</p> <ul style="list-style-type: none"> ▪ Aggiornate per allinearle agli standard PCI DSS. ▪ Aggiunto il termine “<i>dati di account</i>” e forniti ulteriori dettagli su “<i>dati del titolare di carta</i>” e “<i>dati sensibili di autenticazione</i>”. ▪ Chiarito che il PAN (primary account number) è il fattore di definizione per l'applicabilità degli standard PCI DSS. ▪ Aggiunto paragrafo (sostituiva la precedente nota a piè di pagina) ed aggiornata la tavola per chiarire che gli elementi di dati devono essere resi illeggibili in conformità al Requisito 3.4 PCI DSS. 	Chiarimento
Aspetti generali	Aspetti generali	<p>Istruzioni e contenuto per il rapporto di convalida</p> <p>Aggiunti criteri di reporting se un requisito non si applica ad una determinata applicazione di pagamento, alla parte 3.</p>	Chiarimento
Aspetti generali	Aspetti generali	<p>Operazioni di completamento del programma PA-DSS</p> <p>Aggiornato riferimento all'attestato di convalida.</p>	Chiarimento
Tutti i requisiti	Tutti i requisiti	<p>Colonna Requisiti in tutto lo Standard</p> <p>Riscritta, con parole diverse, ogni nota in cui in precedenza si segnalava “<i>Requisito X.X PCI Data Security Standard</i>” utilizzando “<i>In linea con il Requisito X.X PCI DSS</i>” per chiarire l'allineamento tra gli standard PCI DSS e PA-DSS.</p>	Chiarimento
Tutti i requisiti	Tutti i requisiti	<p>Requisiti e procedure di test in tutto lo Standard</p> <p>Ogni volta che in precedenza si indicava di verificare un requisito PA-DSS “<i>in conformità al Requisito X.X PCI DSS</i>”, il requisito e le procedure di test corrispondenti sono stati importati dallo standard PCI DSS e riscritti con parole diverse come applicabile alle applicazioni di pagamento.</p>	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
1.1	1.1	<p>Requisito e procedure di test</p> <ul style="list-style-type: none"> ▪ Aggiunta nota per chiarire che per emittenti e società che supportano servizi di elaborazione di emissione è ammissibile memorizzare dati sensibili di autenticazione in presenza di una giustificazione aziendale e di una memorizzazione sicura dei dati. ▪ Aggiunto test 1.1.a per emittenti e società che supportano servizi di emissione per verificare che l'applicazione di pagamento è destinata solo ad emittenti e/o società che supportano i servizi di emissione. ▪ Spostata la procedura di test in precedenza numerata 1.1 a 1.1.b, inserendo prima <i>“Per tutte le altre applicazioni di pagamento”</i>. 	Chiarimento
1.1.1	1.1.1	<p>Requisito e procedura di test Modificato <i>“in un chip”</i> con <i>“dati equivalenti contenuti in a chip”</i>.</p>	Chiarimento
1.1.1 – 1.1.3	1.1.1 – 1.1.3	<p>Requisiti e procedure di test Eliminati i riferimenti specifici al Glossario in quanto in tutto lo standard sono presenti altre parole del glossario per le quali non si viene fatto alcun riferimento allo stesso.</p>	Chiarimento
1.1.1 – 1.1.3	1.1.1 – 1.1.3	<p>Procedure di test Chiarito che il test deve comprendere l'esame di <i>“almeno i seguenti tipi di file di dati”</i>.</p>	Chiarimento
2.1	2.1	<p>Procedura di test Chiarito che l'identificazione di tutte le posizioni dei dati dei titolari di carta deve comprendere le istruzioni per la configurazione del software sottostante per impedire l'acquisizione o la conservazione involontaria di dati dei titolari di carta.</p>	Chiarimento
2.3	2.3, 2.3.a – 2.3.e	<p>Requisito e procedure di test</p> <ul style="list-style-type: none"> ▪ Chiarito che il requisito è valido solo per il PAN. ▪ Eliminata nota sull'informazione minima sull'account poiché ciò è stato chiarito nel requisito e nella tabella di applicabilità PCI DSS. ▪ Chiariti i requisiti in caso di utilizzo di hashing o troncatura per rendere il PAN illeggibile. ▪ Aggiunta nota per identificare il rischio di PAN in versione hash o troncata nello stesso ambiente e che ulteriori controlli di sicurezza sono necessari per garantire l'impossibilità di ricostruire i dati del PAN originale. ▪ Importate le procedure di test da PCI DSS per creare nuove Procedure da 2.3.a a 2.3.e. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
2.4	2.4, 2.4.a – 2.4.c	Procedure di test Eliminato riferimento a PCI DSS ed importate e riscritte con altre parole le procedure di test PCI DSS per creare nuove Procedure da 2.4.a a 2.4.c, come applicabile alle applicazioni di pagamento.	Chiarimento
2.5	2.5, 2.5.a – 2.5.c	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che ogni chiave usata per rendere sicuri i dati dei titolari di carta deve essere protetta da divulgazione e uso improprio. ▪ Aggiunta nota per chiarire come questo requisito si applica alle KEK (key-encrypting key), se utilizzate. ▪ Eliminato riferimento a PCI DSS ed importate e riscritte con altre parole le procedure di test PCI DSS per creare nuove Procedure da 2.5.a a 2.5.c, come applicabile alle applicazioni di pagamento. 	Chiarimento
2.6	2.6, 2.6.1 – 2.6.7	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Eliminato riferimento a PCI DSS ed importate e riscritte con altre parole le procedure di test PCI DSS per creare nuovi Sottorequisiti e Procedure da 2.6.1 a 2.6.7, come applicabile alle applicazioni di pagamento. ▪ Aggiunta documentazione della <i>Guida di implementazione del programma PA-DSS</i> alla Procedura di test 2.6.a e rinumerata la precedente procedura 2.6.a in 2.6.b. 	Chiarimento
2.7	2.7	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che con la precedente formulazione per eliminazione sicura si intende uno strumento o un processo che rende irrecuperabili le chiavi di crittografia o il materiale memorizzato da versioni precedenti dell'applicazione di pagamento. ▪ Aggiunto <i>“eliminazione di una KEK (key encryption key)”</i> come esempio per rendere irrecuperabili materiali di chiavi di crittografia o crittogrammi. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
3.1	3.1, 3.1.1 – 3.1.10	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Eliminato riferimento a PCI DSS ed importate e riscritte con altre parole le procedure di test PCI DSS per creare nuovi Sottorequisiti e Procedure da 3.1.1 a 3.1.10, come applicabile alle applicazioni di pagamento. ▪ Chiarito che l'autenticazione sicura deve essere applicata a tutti gli account, generati o gestiti dall'applicazione, al completamento dell'installazione e per le sue successive modifiche. 	Chiarimento
3.1.a – 3.1.c	3.1.a – 3.1.d	Procedure di test <ul style="list-style-type: none"> ▪ Spostata procedura di test 3.1.c a 3.1.a per soddisfare la documentazione della <i>Guida per l'implementazione del programma PA-DSS</i> e chiariti i contenuti per essere in linea con i sottorequisiti importati. ▪ Spostata la procedura di test 3.1.a a 3.1.d per allinearla ai sottorequisiti importati e aggiunto chiarimento per verificare con test la presenza dell'autenticazione sicura al completamento dell'installazione e dopo le modifiche successive. ▪ Aggiunta nuova Procedura di test al punto 3.1.c, per verificare con test che l'applicazione di pagamento applica le modifiche agli account predefiniti. 	Chiarimento
3.2	3.2	Requisito Chiarito che questo requisito si occupa delle istruzioni del fornitore per i clienti.	Chiarimento
4.1	4.1, 4.1.a – 4.1.b	Procedure di test Spostata la procedura di test da 4.2.b a 4.1.b per allinearla ai requisiti riorganizzati. Formulazione leggermente modificata per chiarezza.	Chiarimento
4.2	4.2, 4.2.1 – 4.2.7	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Fatta chiarezza in relazione a informazioni specifiche da inserire nei file di log. ▪ Eliminato riferimento a PCI DSS ed importate e riscritte con altre parole le procedure di test PCI DSS per creare nuovi Sottorequisiti e Procedure da 4.2.1 a 4.2.7, come applicabile alle applicazioni di pagamento. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
4.2	4.3, 4.3.1 – 4.3.6	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Fatta chiarezza in relazione a informazioni specifiche da inserire nei file di log. ▪ Eliminato riferimento a PCI DSS (in precedenza in 4.2) ed importate e riscritte con altre parole le procedure di test PCI DSS per creare Requisito, Sottorequisiti e Procedure nuovi da 4.3.1 a 4.3.6, come applicabile alle applicazioni di pagamento. 	Chiarimento
N/A	4.4	Nuovo requisito e procedure di test Aggiunto nuovo requisito per rendere necessario che le applicazioni di pagamento facilitino la generazione centralizzata di registri, in linea con il requisito 10.5.3 PCI DSS.	Requisito in evoluzione
5.1	5.1	Requisiti e procedure di test Aggiornati per allinearli al Requisito 6.3 PCI DSS.	Chiarimento
5.1.1	N/A	Requisiti e procedure di test Eliminato 5.1.1 in quanto i test di vulnerabilità vengono ora presi in esame da 5.2.1 a 5.2.9.	Chiarimento
5.1.2 – 5.1.3	N/A	Requisiti e procedure di test Eliminato per chiarezza in quanto l'ambiente di produzione non è applicabile agli sviluppatori di applicazioni ai fini del programma PA-DSS.	Chiarimento
5.1.1 – 5.1.7	5.1.1 – 5.1.4	Requisiti e procedure di test Rinumerati a causa dell'eliminazione dei precedenti Requisiti da 5.1.1 a 5.1.3.	Chiarimento
5.1.4	5.1.1	Procedura di test Eliminato il contenuto <i>“oppure sono modificati prima dell'uso”</i> per chiarire lo scopo.	Chiarimento
5.1.5	5.1.2	Requisito e procedura di test Chiarito che account e dati dei test devono essere eliminati prima della <i>“distribuzione al cliente”</i> .	Chiarimento
5.1.7	5.1.4	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Consolidate le procedure di test (in precedenza 5.1.7.a e 5.1.7.b) in un'unica procedura 5.1.4.a, per combinare in una singola procedura le applicazioni "interna" e "Web", ed eliminata la procedura di test in precedenza 5.1.7.b diventata ora superflua. ▪ Eliminato il riferimento specifico alle applicazioni Web ed alla Guida OWASP per consolidare i requisiti di codifica sicura per le applicazioni comprese nell'ambito, incluse le applicazioni non Web. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
5.2	5.2	Requisito e procedure di test <ul style="list-style-type: none"> ▪ Chiarimento che i requisiti per la codifica sicura e la prevenzione delle vulnerabilità si applicano a tutti i tipi di applicazioni sviluppate per i clienti incluse nell'ambito, piuttosto che solo alle applicazioni Web. ▪ Eliminata la dipendenza da OWASP ed inseriti altri esempi del settore SANS CWE e CERT. 	Chiarimento
5.2.1 – 5.2.10	5.2.1 – 5.2.9	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Vulnerabilità in precedenza da 5.2.1 a 5.2.10 aggiornate e combinate con il precedente requisito 5.1.1 per riflettere le attuali istruzioni di CWE, CERT e OWASP. ▪ Requisiti da 5.2.7 a 5.2.9 individuati come vulnerabilità specifiche per le applicazioni Web. 	Chiarimento
N/A	5.2.6	Requisito e procedura di test Aggiunto nuovo requisito 5.2.6 per prendere in esame le vulnerabilità di rischio elevato individuate al 7.1.	Requisito in evoluzione
5.3.2	5.3.2	Requisiti e procedure di test Modificati il requisito e la procedura di test per chiarire la necessità di approvazione concessa dalle parti autorizzate piuttosto che dal "management".	Chiarimento
5.3.3	5.3.3, 5.3.3.a – 5.3.3.b	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Chiarito lo scopo di requisito e procedura di test 5.3.3.a per test di funzionalità intesi ad accertare che le modifiche non influiscano negativamente sulla sicurezza del sistema. ▪ Il precedente Requisito 5.1.1 viene incorporato nella nuova Procedura di test 5.3.3.b, per prendere in esame il test delle modifiche con riferimento a 5.2. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
5.4	5.4	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Chiarito che solo i servizi, protocolli, daemon ecc. sicuri e necessari devono essere attivati e le funzioni di sicurezza implementate per ogni tale servizio o altro elemento non sicuro. ▪ Separata la Procedura di test 5.4 in singole Procedure 5.4.a e 5.4.b ed illustrata con maggiore chiarezza la Procedura di test 5.4.b per garantire che ogni servizio necessario sia configurato pronto per l'uso. ▪ Aggiunta Procedura di test 5.4.c per verificare che la <i>Guida per l'implementazione del programma PA-DSS</i> documenti tutti i necessari protocolli, servizi, componenti e software e hardware dipendenti. 	Chiarimento
6.1	6.1, 6.1.a – 6.1.f	Procedure di test <ul style="list-style-type: none"> ▪ Eliminato riferimento a PCI DSS ed importate le procedure di test PCI DSS per creare le nuove Procedure di test da 6.1.a a 6.1.f, come applicabile alle applicazioni di pagamento. ▪ Aggiornata Procedura di test 6.1.f per chiarire le istruzioni da inserire nella <i>Guida per l'implementazione del programma PA-DSS</i>. 	Chiarimento
6.2	6.2	Requisiti e procedure di test <ul style="list-style-type: none"> ▪ Aggiornata nota relativa all'uso di WEP a partire dal 30 giugno 2010. ▪ Eliminato il riferimento a PCI DSS nella Procedura di test 6.2.b e chiariti gli elementi per l'inserimento nella <i>Guida per l'implementazione del programma PA-DSS</i>. 	Chiarimento
7.1	7.1, 7.1.a – 7.1.d	Requisiti e procedure di test Aggiornato requisito per garantire che le vulnerabilità identificate siano classificate in funzione del rischio. Aggiunta procedura di test 7.1.a per allinearla al requisito. Separata la precedente procedura di test 7.1 in singole procedure da 7.1.a a 7.1.d.	Requisito in evoluzione
7.2.a – 7.2.b	7.2.a – 7.2.e	Procedure di test Separata la procedura di test 7.2.a in singole procedure da 7.2.a a 7.2.d. Rinumerata la precedente procedura di test 7.2.b in 7.2.e.	Chiarimento
10, 11	10	Requisiti e procedure di test Uniti i Requisiti 10 e 11 per eliminare inutili ripetizioni. Il Requisito originale 10.1 è ora il Requisito 10.3.1.	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
10, 11	10	<p>Requisiti e procedure di test</p> <ul style="list-style-type: none"> ▪ Rinumerato il precedente 11.1 in 10.1. Chiarito che l'applicazione di pagamento non deve interferire con l'uso di tecnologie di autenticazione a due fattori per accesso remoto sicuro. Aggiornato esempio a <i>"Radius con token"</i>. ▪ Rinumerato il precedente 11.2 in 10.2. Nessuna modifica al contenuto. ▪ Aggiunto Requisito originario 10.3 per accesso remoto nell'applicazione di pagamento. Precedenti requisiti 10.1 e 11.3 rinumerati rispettivamente in 10.3.1 e 10.3.2. Nessuna modifica al contenuto. ▪ Spostati esempi dalle procedure di test alla colonna dei requisiti. 	Chiarimento
12, 13, 14	11, 12, 13	<p>Requisiti e procedure di test</p> <p>Precedenti requisiti 12, 13 e 14 rinumerati rispettivamente in requisiti 11, 12 e 13 a seguito dell'unione dei requisiti 10 e 11.</p>	Chiarimento
12.1	11.1	<p>Requisiti e procedure di test</p> <ul style="list-style-type: none"> ▪ Inclusa SSH come esempio di protocollo di sicurezza, eliminati gli esempi dalla procedura di test. ▪ Spiegazione della <i>terminologia "protocolli di crittografia e sicurezza avanzati"</i>, per congruenza. 	Chiarimento
12.2	11.2	<p>Requisiti</p> <p>Chiarito che questo requisito si applica se l'applicazione di pagamento facilita l'invio di PAN mediante tecnologie di messaggistica degli utenti finali e che la soluzione deve rendere illeggibile il PAN oppure implementare la crittografia avanzata.</p>	Chiarimento
13.1	12.1	<p>Requisiti e procedure di test</p> <p>Spiegazione della <i>terminologia "protocolli di crittografia e sicurezza avanzati"</i>, per congruenza.</p>	Chiarimento
Appendice A	Appendice A	<p>Tutti i requisiti</p> <ul style="list-style-type: none"> ▪ Aggiornato contenuto per la <i>Guida per l'implementazione del programma PA-DSS</i> per riflettere i cambiamenti apportati nei Requisiti PA-DSS. ▪ Aggiornati riferimenti a PCI DSS per riflettere i requisiti PA-DSS. 	Chiarimento

Sezione o Requisito		Modifica	Tipo ⁱ
Vecchio	Nuovo		
Appendice B	Appendice B	Punto 5.b Aggiunte procedure di laboratorio "back" che erano state erroneamente omesse dalla versione precedente.	Chiarimento
Appendice B	Appendice B	Punto 6.b Aggiornato riferimento per vulnerabilità per evitare di fare affidamento solo su OWASP, come da modifiche apportate ai Requisiti 5.1 e 5.2 PA-DSS.	Chiarimento
Appendice B	Appendice B	Punto 7.c Aggiunto chiarimento che il PA-QSA deve convalidare l'installazione completa dell'ambiente di laboratorio remoto per garantire l'effettiva simulazione da parte dell'ambiente di una situazione del mondo reale.	Chiarimento
Appendice C	Attestato di convalida	Tolto dall'Appendice Riorganizzato il formato per fornire le informazioni del fornitore dell'applicazione prima delle informazioni del PA-QSA.	Chiarimento

ⁱ Spiegazioni di "Tipo":

Nuovo tipo	Vecchio tipo	Definizione
Chiarimento	Chiarimento	Maggiori informazioni sullo scopo del requisito. Assicurare che la formulazione sintetica negli standard presenti lo scopo dei requisiti che si desidera.
Ulteriori istruzioni	Spiegazione	Spiegazioni e/o definizioni per fornire una migliore comprensione o ulteriori informazioni su un determinato argomento.
Requisito in evoluzione	Miglioramento	Modifiche per assicurare che gli standard siano aggiornati alle minacce emergenti ed ai cambiamenti del mercato.